Chapter Thirteen

ETHICS AND INFORMATION WARFARE

John Arquilla

War forms an integral part of the history of mankind, alternately driving civilization forward, then imperiling it. A natural ambivalence toward war has thus developed, with its acceptance as a necessary evil tempered by vigorous, sustained efforts to control its frequency and intensity. Thus, from the dawn of the recorded history of conflict, attempts have been made to craft an ethical approach to war. They break down into two categories: a set of guidelines regarding going to war at all and a set of strictures by which combatants, should they adhere to them, might fight during a war in a just manner. These dimensions of the ethical approach to war have received searching scrutiny. In this early period of the information age, the time has come to revisit these ethical concepts, as new forms of conflict are emerging to test existing understanding of "just wars"—much as advanced information technologies are already requiring a rethinking of a wide range of commercial and criminal laws.

Another reason to devote some attention to ethical issues and future conflict is that, in the mountainous sea of literature on information warfare, little attention has been given thus far to its ethical dimensions.[1] Part of the problem is that information warfare is itself a multifaceted concept—in Martin Libicki's phrase, "a mosaic of forms." (Libicki, 1996, p. 6.) Information warfare is a concept that ranges from the use of cyberspace to attack communication nodes

[1] A very thoughtful early discussion of the legal dimensions of information warfare can be found in Aldrich (1996). Also, see Schwartau (1996).

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **1999**	2. REPORT TYPE	3. DATES COVERED **00-00-1999 to 00-00-1999**

4. TITLE AND SUBTITLE **Ethics and Information Warfare**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Graduate School of Operational and Information Sciences,Department of Defense Analysis,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Strategic Appraisal: The Changing Role of Information in Warfare (Zalmay Khalilzad, John P. White, and Andrew Marshall eds.), Santa Monica, CA: RAND, 1999

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

and infrastructures to the use of information media in the service of psychological influence techniques. Because it constitutes such a variety of conflict modes, information warfare poses problems for those who seek out ethical guidelines for its waging.

This subject is of importance to Americans, from civilian and military leaders to the mass public. Information warfare, as it evolves, is demonstrating a growing disruptive capacity, both against classic military command and control nodes and against many elements of the national information infrastructure. Quite simply, the United States, whose society has grown dependent upon advanced information technologies, has the most to lose from a wide-ranging information war—and thus has an interest in preventing its outbreak. A well-informed ethical approach to the burgeoning problem of information warfare may even demonstrate that it is possible, in this case, to do good and to do well. Indeed, an ethical approach to conflict in the information realm may swiftly prove as practically useful and valuable—even when the opponent is a nonstate criminal or terrorist organization—as it is morally desirable.

This chapter draws from historical notions of ethics and war and applies them to the phenomenon of information warfare. First, the key concepts of just war theory are explained, and a functional definition of information warfare is developed. Next, the various ethical formulations are appraised in light of information-age effects on the conduct of warfare. Last, insights are drawn from this analysis, and guidelines for "just" information warfare are advanced.

CONCEPTS AND DEFINITIONS

A remarkable consistency characterizes thinking about just wars, from ancient to modern times. Thus, nearly three millennia ago, concerns were advanced about the need for an ethical approach to going to war, as well as to waging war. For example, the ancient Greek geographer, Strabo, observed that, in the War of the Lelantine Plain (circa 700 BCE), all parties agreed to ban the use of "projectile missiles" because they constituted an ethically repugnant form of war. The Greeks were also concerned about honoring treaties and conventions and about avoiding undue brutality. (Ober, 1994.) These notions track very closely with the Thomist paradigm, developed in the Middle Ages, which still dominates thinking about ethics and conflict.[2]

The Concepts of Just War Theory

The key concepts of just war theory fall into the categories of criteria for going to war *(jus ad bellum)* and fighting justly during war (*jus in bello*):

Tenets of Just War (*Jus ad Bellum*)

A. *Right Purpose.* Justifiable reasons for going to war revolve around the concept of self-defense. Notions of right purpose generally include such ideas as preemption (i.e., striking in anticipation of an oncoming attack), but are less open to the idea that preventive war (i.e., striking at a propitious time) is just.[3] Also, this category excludes wars of conquest or annexation.

B. *Duly Constituted Authority.* It is clear from all the literature on ethics and war that a necessary condition for having a just war is that the decision to fight must come from a government—not from an individual. Wars waged by individuals have always fallen outside the law, the best example being provided by 19th-century prohibitions on the practice of private wars, or "filibusters," as they were then known.

C. *Last Resort.* Simply put, war cannot be considered just unless it follows exhaustive pursuit of negotiations and other means of conflict resolution. A good example of this is given in Thucydides' depiction of the extended crisis-bargaining between Athens and Sparta as both sides sought in vain to

[2] See Thomas Aquinas, *Summa Theologica*, especially Book II, Part II. Ramsey (1961) remains a classic exposition of the Thomist view of just war. On just war theory during this period, see also Russell (1975).

[3] It should be noted that ideas about "right purpose" in the nuclear era have retained self-defense as an ethical construct, while preemption is viewed as unacceptable—though not without some dissent. Preventive nuclear war, though seriously contemplated in the late 1940s and early 1950s to preserve the U.S. monopoly on atomic weapons, is very nearly unanimously considered ethically unacceptable. On these issues, see Rosenberg (1994).

head off the oncoming Peloponnesian War.[4] The run-up to the Gulf War sounded many echoes of these ancient events.

Concepts of Just Warfighting (*Jus in Bello*)

D. *Noncombatant Immunity.* Wherever and whenever possible, according to just war theory, those waging the war must strive to avoid harming civilians or enemy troops that have surrendered. Fleeing troops that have no ability to fight (e.g., the Iraqi troops retreating along the "highway of death") fall into a gray area ethically, attacks upon them being allowed—but not encouraged.[5] Conventional aerial bombing and, later, nuclear war, have posed problems for the notion of noncombatant immunity that remain unresolved. One attempt to cope with this was by considering air and nuclear attacks on strategic targets as permissible, with civilian losses treated as "collateral." (Walzer, 1977, pp. 255–260.)[6]

E. *Proportionality.* There are several aspects to this notion.[7] First, and best known, is the issue of using force in a manner

[4] Thucydides, *The History of the Peloponnesian War,* Book I, Chs. 1–4. See also Kagan (1994).

[5] On this point, Walzer (1977), p. 129, notes that the rule of thumb is to limit "excessive harm." Yet, he observes that many have argued that this restriction can be relaxed if such action contributes clearly and materially to victory.

[6] Also, it should be noted that strategic aerial bombardment has just as often been used deliberately to terrorize civilians, being considered a key element of deterrence stability and coercive diplomacy. See Quester (1966) and Pape (1995). The willingness of nuclear strategists to accept the likelihood of some "collateral" civilian losses grows, in part, out of the perceived need to strike an adversary in time to disrupt his own oncoming attack (preemption), or to strike early enough that the enemy will not be able even to develop a threatening capability of his own (prevention)—as in the case of the 1981 Israeli raid on the Iraqi nuclear weapon program at Osiraq.

[7] Johnson (1981), pp. xxii–xxiii, observes that the concept of proportionality falls under both *jus ad bellum* and *jus in bello.* In the former case, the author argues that proportionality refers to "doing more harm than good." In the latter, he suggests limits on the kinds of weapons that may be used. For purposes of this study, proportionality is considered as described in E, above, because this captures much of both of Johnson's notions. Further, the idea of doing more harm than good has been considered part of the notion of *jus in bello,* as this is a calculation more possible to make during, rather than prior, to a war—save perhaps with the exception of nuclear war, whose catastrophic consequences for all were never doubted.

avoiding excessive application. A second facet, though, might be that this concept requires ensuring that a sufficient proportion of one's forces, relative to the adversary, are employed, so as to enhance the probability of winning. Thus there is a built-in tension between the need for "enough," but not "too much," force. Finally, the term is often used to mean response in kind, or in a tit-for-tat fashion.[8]

F. *More Good Than Harm*. This is a concept from the Thomist paradigm. This notion implies, of warfighting, that ethical conduct requires calculation of the net good to be achieved by a particular use of force. An example of such a calculation, though clouded by violation of notions of noncombatant immunity, is Truman's decision to drop the atomic bomb on Hiroshima to avoid a more costly conventional invasion of Japan.

As one considers these ethical constructs, it appears that ideas about the second broad category, just warfighting, might also form part of the calculations for going to war in the first place. Thus, they should all be seen as interrelated aspects of just war theory. However, from an ethical perspective, it seems clear that responding to the *ad bellum* factors must be considered a primary duty of those who would make decisions about war and peace. The *in bello* factors, while related to decisions regarding conflict initiation, should be seen, in ethical terms, as lying within the realm of decisionmakers' secondary duties.[9]

The six facets described above cover most of the conceptual ground, and they should allow for analysis of any latent tensions between duty- and utility-based ethics; the potential for escalation from

[8] For a modern perspective on the concept of proportionality, see Schelling (1966), who makes the important point that a proportional retaliation for an attack need not use means that are identical to those employed by an aggressor.

[9] The author is grateful to Tora Bikson for pointing out that just war theory, as subdivided above, may be categorized in terms of the classical ethical notions of primary and secondary duty. This notion is apparent in the essays on ethics of Bentham, Kant, and others and is examined in detail in Moore (1993). The notion of duty is also an element in Rawls (1971). However, the conflicts inherent in striving to reconcile sometimes conflicting duties to "fairness" can be considerable, as argued in Alejandro (1997).

information warfare to conventional, or even nuclear, war; and the prospects for some form of operational arms control.[10] The need now, though, is to consider how this multidimensional definition of just war theory fits with current notions of information warfare.

Defining Information Warfare

To consider the ethical dimensions of information warfare, it is first crucial that the phenomenon be classifiable as a true form of war, as opposed to being just a manifestation of criminal or terrorist activity—or an extension of covert psychological operations or intelligence-oriented activities. With this in mind, it is useful to note that, in the several years since the introduction of information warfare, the concept has evolved and broadened to include activities that, while information-driven, are not considered warfare and therefore do not invoke the ethical concepts of just war theory.

To separate these two classes of activities, a broad view has emerged, in which the term *information operations* refers to the entire range of information-intensive interactions across a spectrum that includes psychological operations; perception management; information security; and, of course, information warfare. Use of "information operations" thus allows us to reserve the term information warfare for a specific subset of warlike activities, all of which invoke just war theory.

Of what, then, does information warfare consist? Principally, this form of war concerns striking at communication nodes and infrastructures. The weapons used in such attacks are generally thought to be those employable via cyberspace (e.g., logic bombs, computer viruses). However, information warfare also includes the use of a variety of other offensive tools, from conventional explosives to high-

[10] Operational arms control consists of constraints on behavior (e.g., on the movement or exercise of troops at certain times and places or the agreement not to use certain types of weapons, such as chemicals, land mines, or dumdum bullets). Structural arms control refers to limiting, reducing, or eliminating the actual quantities of weapons and, for the present, seems to lie beyond the ability to control in this fashion—given the ease of production and diffusion of information weapons. Yet, technological advances do hold out the prospect for improving surveillance to a point where structural arms control of weapons of information warfare may become feasible.

power microwave weapons, that can also be used to strike at information-rich targets.

Attacks on information-rich targets using conventional weapons, while undoubtedly an integral part of information warfare, present few ethical novelties because they have long been a part of warfare. Therefore, this chapter will focus on the ethical implications of the new forms of warfare implicit in information warfare, particularly the weapons employable via cyberspace.

The range of operations that might make use of information warfare extends broadly, from the battlefield to the enemy home front. Thus, information warfare may serve as a form of close-support for military forces during active operations. It may also be employed in strategic campaigns designed to strike directly at the will and logistical support of an opponent. The last notion of information warfare, in which it may be pursued without a prior need to defeat an adversary's armed forces, is an area of particular interest.[11] In many respects, it resembles notions of the strategic uses of airpower that emerged in the 1920s and 1930s and merits, therefore, close scrutiny from an ethical perspective—much as air warfare was the focus of serious ethical debate prior to and during World War II.[12]

Although it may bear a strategic resemblance to airpower, information warfare has a quite different set of effects and properties. While airpower can generally perform much destruction on fixed points (e.g., in World War II, on U-boat pens and ball-bearing plants),[13] information attacks, even using conventional weapons, inflict far less destruction.[14] Rather, the effects of information attacks are disrup-

[11] For an exposition of this view, see Molander, Wilson, and Riddile (1996).

[12] Garrett (1993) provides an excellent summary of the debate about the ethics of airpower. For a good discussion of strategic aerial bombardment as an autonomous tool of war, including skeptical French and cautious British views, see Quester (1966), pp. 50–70.

[13] The discussion here is limited to the effects of airpower using conventional explosives, as opposed to weapons of mass destruction.

[14] "Destruction" should be considered a multidimensional concept. First, there is the physical "burnout" of computers, power lines, system controls, etc. Then there is the erasure or corruption of data. Finally, there is loss of life (e.g., crash of an airliner due to a disrupted air traffic control system) and environmental damage (e.g., an oil

tive, and may occur over wide areas (e.g., knocking out a geographic power grid), even in the face of defensive redundancies emplaced in anticipation of information-warfare attacks. Another difference is that, while strategic aerial bombardment inevitably causes civilian losses, even with today's guided weapons, information weapons will lead to far fewer deaths—despite the widespread disruptive effects. This lower lethality and destructiveness may make the damage done by information-warfare attacks somewhat harder to assess accurately—and may complicate calculations designed to craft a proportional response.

Thus, strategic information weapons have area effects that, in some respects, extend quite a bit further than even weapons of mass destruction—but with "mass disruption" being their hallmark. And it is just this prospect of having wide effects without causing very many deaths or dire environmental consequences that makes information warfare such a potentially attractive form of conflict. Although the existence of these capabilities is the subject of some debate, it is assumed for the purposes of this study that such capabilities either already exist or soon will.

Finally, it is important to note the inherent blurriness with regard to defining "combatants" and "acts of war." In strategic aerial bombardment, it is quite clear who is making the attacks. It is also clear that the enemy combatants are its military forces. This latter notion is relaxed a bit in guerrilla warfare, in which civilians often engage in the fighting. But in information warfare, almost anyone can engage in the fighting. Thus, it is important, from an ethical perspective, to make a distinction between those with access to advanced information technology and those using it for purposes of waging information warfare. Further, the nature of cyberspace-based attacks is such that there may often be an observational equivalence between criminal, terrorist, and military actions. The ethical imperative that attaches to these concerns is the need to determine the identity of the perpetrators of information-warfare attacks and to make a distinction between sporadic depredations and actions that form part of a recognizable campaign in pursuit of discernible aims.

pipeline spill resulting from disruption of automated system controls) to round out the concept of destruction.

JUST WAR THEORY AND INFORMATION WARFARE

Armed with the six tenets of just war theory and the pared-down definition of information warfare described above, one may now relate them to each other to determine the extent to which information warfare can be said to be just or can be waged justly. This form of analysis allows for a survey of the ethical issues—and elicits some surprising results.

Jus ad Bellum

In the realm of going to war ethically, the concept of "right purpose" does not appear to be put under much stress. Self-defense and preemption, both allowed under classical just war theory, may have new dimensions because of information warfare, as they may be applied more promptly with disruptive information weapons. The one area that may change is that of the use of force in preventive ways. Under existing just war theory, prevention (i.e., striking to prevent the rise of a threat, like the Israelis at Osirak in 1981) lies on tenuous ground. But information warfare might prove especially useful in derailing the rise of a threatening power—particularly the forms of information attack that might be useful in slowing down a potential adversary's process of proliferation of weapons of mass destruction.

With regard to the second concept, "duly constituted authority," the very nature of information weaponry may introduce new stresses for this long-established ethical concept. For the types of capabilities needed to field an information-warfare campaign—particularly one that is waged principally in cyberspace—there is little need for the levels of forces required in other forms of war. Therefore, the state monopoly on war reflected in the concept of duly constituted authority will likely be shaken, as nonstate actors rise in their ability to wage information warfare. This may be part of an overall phenomenon in which the information revolution is causing a diffusion of power away from states and toward nonstate actors—both peaceful, civil society elements and the new "uncivil society" of information-age terrorists and transnational criminal organizations.[15] Finally, this rise of new nonstate actors capable of waging

[15] On these issues, see Hoffman (1997) and Williams (1994).

information warfare may also encourage states to employ them. Indeed, nonstate actors will likely prove useful cutouts that help to maintain deniability, or ambiguity, about the ultimate identity of an adversary. This suggests the possibility that quite weak states may thus be allowed to strike at the strong, given the lessened likelihood that they will be discovered and subjected to retaliation. However, this problem might be mitigated by improvements in cyberspace-based detection, surveillance, and tracking technologies.

This ease of entry into the realm of information warfare not only erodes the strictures against acting without duly constituted authority. It also suggests that the convention regarding going to war only as a last resort will come under strain. For information warfare, though it may disrupt much, at great cost to the target, does little actual destruction—and will likely prove a form of warfare that results in only incidental loss of life. In this respect, information warfare can be viewed as somewhat akin to economic sanctions as a tool of coercion (though probably less blunt an instrument than an embargo). This similarity should also contribute to the erosion of the last-resort principle. However, as with economic sanctions, certain nonlethal parts of information warfare may not be considered acts of war and thus may be exempt from just war considerations—a status that would increase the likelihood of their use but would preserve the integrity of the last-resort principle for actions deemed acts of war.

Finally, in the case that all information-warfare actions are considered acts of war, if information warfare's low destructiveness is coupled with a situation that features self-defensive "right purpose"—say, in a crisis where skillful preemption might head off a general war—the normative inhibition against early uses of force will erode even further.

Jus in Bello

With regard to the issue of waging information warfare justly, there are also many ways in which the classical concepts will come under pressure. First, one approach to information warfare concentrates on striking an adversary's transportation, power, communication, and financial infrastructures. This must be seen as a kind of war that targets noncombatants in a deliberate manner—because they will suffer from such attacks inevitably and seriously. The purpose of this type of information warfare is to undermine the enemy's will to resist, or to persist, in a particular fight; in this respect, strategic information warfare is very similar to early notions of strategic aerial bombardment that targeted noncombatants.[16]

In the realm of information warfare, it should be noted that, even as planners may be driven to wage a form of war whose effects will be most felt by noncombatants, there is another aspect to strategic attack—one strictly aimed at disrupting the movements and operations of military forces. Information warfare is a sufficiently discriminate tool that making this distinction is possible—and just war theory implies eschewing the targeting of noncombatants and focusing instead upon purely military targets and effects. Thus, an apparently quite attractive coercive tool of force (strategic information warfare) runs hard up against the enduring ethical constraints against attacking noncombatants. This dimension of just war theory may, therefore, pose the most nettlesome policy dilemma—and may require the most creative solution.

Another thorny issue is posed by the just warfighting concept of proportionality, whose major concern is with avoiding the use of excessive force during a conflict. In one respect, the discriminate use of information warfare should make it possible to wage war quite proportionately. That is, it should be possible to respond to information-warfare strikes by some adversary in a very precise, tit-for-tat fashion, neatly calculated and calibrated. However, two problems might emerge that put notions of proportionality under some stress. First, information-warfare attackers might strike at an opponent's critical infrastructures, but have few of their own that could be retaliated against by means of information warfare. This prompts the question of when more traditional military measures—including some amount of lethal force—might be used in response to information-warfare attacks without violating notions of proportionality.

[16] See Douhet (1942) and De Seversky (1942). Warden (1989) is a clear throwback to Douhet and De Seversky. On the other hand, nuclear strategists did strive hard to limit noncombatant losses, by developing the concept of counterforce targeting. But this palliative was seen as still allowing massive, civilization-endangering casualties. On this point, see Ball and Richelson (1986).

Another problem might arise if the defender, or target, were struck by information-warfare attack and had little or no means of responding with information weaponry. Russian strategic thinkers have considered this last issue, with some of their analysts ending up recommending forceful responses—even to the extent of threatening a renewed form of "massive retaliation" with weapons of mass destruction against information-warfare attackers. In this respect, Schelling's suggestion that varied responses can solve one dilemma of proportionality may engender a new dilemma: the asymmetrical retaliatory response may tend toward escalation. A prime example of the sort of problem that can arise is Russian declaratory policy toward information-warfare attacks. As one Russian defense analyst put it recently:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of conflict, whether there were casualties or not. . . . considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces. Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself. (Tsymbal, 1995.)[17]

Thus, Thomas Schelling should be seen as providing some guidance in these issue areas, but his solution poses difficulties and risks. He has noted that proportionality is a reasonable principle, one that need not be considered to require the use of identical weaponry when one is engaging in retaliation. He also implicitly argues that the risk escalatory threats pose is not necessarily credible. See, for example, his assessment of the 1950s U.S. policy of massive nuclear retaliation as a concept that "was in decline almost from its enunciation." (Schelling, 1966, p. 190.) Yet the massive retaliatory threat may be the only credible deterrent that a potential victim of information warfare may be able to pose. Aside from deliberately disproportionate responses, there is also the problem that gauging the

[17] Thomas (1997), pp. 76–77, reinforces the point that the Russians see the information-warfare threat as "real, and intensifying" and that one perspective is indeed that "Moscow's only retaliatory capability at this time is the nuclear response."

comparability of damage done by radically differing weapon systems (e.g., exploding smart bombs versus computer logic bombs) is going to prove quite difficult. Finally, the problem of perpetrator ambiguity further weakens proportionate response, because one may simply not have enough data to determine just who is responsible for a particular attack.

The last of the just warfighting issues that must be considered is even more nebulous than notions of proportionality. It consists of the admonition to engage in operations that do more good than harm.[18] However, even if difficult to measure or define, this requirement for ethical calculation of costs versus benefits may be eased by the idea that information warfare requires, and effects, but little destruction and will likely lead to scant loss of life. Unlike the terrible dilemma that faced President Truman—a choice between massive immediate casualties inflicted upon the enemy in the near term, versus perhaps greater long-term losses for Japanese and Americans—information warfare may afford the prospect of a use of force that causes little destruction but that might, used properly, help to head off a potentially bloody war.

SOME GUIDELINES FOR POLICY

Based on the foregoing description and analysis of the ways in which notions of information warfare interact with just war concepts, it is now possible to think about establishing a general set of guidelines that will help decisionmakers and information warriors behave as ethically as circumstances allow—or at least to recognize and strive to resolve the apparent tension that arises here between utility- and duty-based ethical guidelines. Rectitude aside, it must also be recognized that war is about winning. Therefore, guidance for policy or doctrine must cope with the dilemmas that may emerge as a result of striving to act properly and taking the pragmatic actions that are likely to lead to victory.

A good example of this sort of problem is provided by the ancient Israelites in their (2nd century, BCE) efforts to break free from domination by the Seleucids, the inheritors of one part of Alexander's

[18] Again, it should be noted that some see this as a *jus ad bellum* issue. See Johnson (1981), p. xxii.

empire. The Hebrew scripture forbade fighting on the Sabbath—so the Greeks soon learned to attack on this day. The slaughters of the rebellious, but observant, Jews that ensued are poignantly lamented: "Let us all die in our innocence. Leaves and earth testify for us that you are killing us unjustly." As the uprising faltered, one of the wise Jewish leaders, Mattathias, perceived the problem and provided an ethical adjustment, in the nick of time, that allowed them at least to defend themselves without violating God's law: "They will quickly destroy us from the earth. Therefore, let us fight against every man who comes to attack us on the Sabbath day." Thus, just warfighting was allowed on the Sabbath—but only *defensive* operations.[19] Soon, the Maccabees won their freedom.

Policy Toward Going to War

The first issue engaged, regarding "right purpose," basically boils down to the question of whether the improved capacity for preventive strikes granted by information warfare can overcome the ethical problems posed by offensive war initiation. The ethical problem deepens when it is recognized that preventive war—striking forcefully before an adversary has serious, threatening capabilities—will generally mean going to war before diplomatic options have been exhausted, that is, not as a "last resort."[20] On the other hand, the basically disruptive rather than destructive nature of information warfare suggests the possibility of a "just warfighting" approach to prevention that eases the ethical dilemma.

Simply put, prevention by means of information warfare might be allowable if (1) strikes were aimed strictly at military targets (e.g., command and control nodes), to avoid or generally limit damage to noncombatants; (2) the amount of suasion employed was enough to deter or substantially slow an attacker, without being so excessive as to have dire economic or social effects; and (3) the good done by pre-

[19] Quotes from 1 Maccabees 2:37–41. This issue was also considered by later Talmudic scholars, notably Gersonides, in his *The Wars of the Lord* (as excerpted in Steinsaltz, 1976). See also the discussion in Steinsaltz (1976), p. 20.

[20] Indeed, the most serious ethical problem with prevention is that the adversary may not even be contemplating going to war, yet he is struck. This dilemma was but one of the considerations—albeit an important one—that led policymakers to decide against striking preventively against either Russia's or, later, China's nascent nuclear capabilities.

venting an adversary from being able to start a particular conflict, or type of conflict, could be said to outweigh the wrong of using force beyond the realm of clearly definable self-defense.[21] Thus, *jus in bello* considerations may be seen as mitigating a serious *jus ad bellum* constraint on information warfare.

The second policy concern, that of remaining within the bounds of notions of duly constituted authority, poses little difficulty from the U.S. perspective, or for any state, for that matter—so long as a state actor refrains from employing a nonstate cutout to wage information warfare on its behalf. The problem goes deeper, though, as the very nature of information warfare implies that the ability to engage in this form of conflict rests now in the hands of small groups and individuals—no longer being the monopoly of state actors. This offers up the prospect of potentially quite large numbers of information warfare–capable combatants emerging, often pursuing their own, as opposed to some state's, policies.

Finally, the just war admonition to engage in conflict only as a last resort must also be examined. Here, the previous discussion of prevention is useful, in that early uses of information warfare may, overall, have some beneficial effects and may not do serious damage to noncombatants. Weighed against this, though, are long-standing normative inhibitions against "going first" in war. For policymakers, the answer is most likely that, as in the nettlesome case of duly constituted authority, so with last resort, there is no easily accepted answer. The rise of nonstate actors implies a serious, perhaps fatal, weakening of this just war constraint; likewise, the ease with which use of information warfare may be contemplated suggests that a sea change will occur with regard to notions of "justice" requiring that war always be undertaken as a last resort. Finally, it may prove possible to relax the ethical strictures about last resort if information-warmakers engaging in early use emphasize disruptive acts—avoiding actions that engender significant destruction.

[21] In this regard, the oft-stated rationales of war initiators, that they were simply starting the war to "defend" their countries against threats that would soon appear, must be viewed with some skepticism. This is the sort of argument Napoleon advanced, feeling he had to conquer all of Europe to defend France, as did German leaders in the first half of this century.

In summary, it appears that policy perspectives on the just initiation of an information war have left a good part of just war theory in tatters. Information warfare now makes preventive war far more thinkable (and practical), straining the limits of the concept of "right purpose." And the manner in which the information revolution empowers small groups and individuals to wage information warfare suggests that the notion of duly constituted authority may also have lost meaning. Finally, the ease in undertaking information-warfare operations, and the fact that they are disruptive, but not very destructive, weakens the notion that justice requires that war be started only as a last resort.

On Just Warfighting

Given the ease with which entry may be made into the ranks of information warfare–capable states and nonstate actors and the attractiveness of targets that primarily serve civilian commercial, transportation, financial, resource, and power infrastructures, the greatest *jus in bello* concern for information warfare may be the problem of maintaining "noncombatant immunity." The number of actors will be (perhaps already is) large and is hardly subject to centralized control. The civilian-oriented target set is huge and is likely to be more vulnerable than the related set of military infrastructures—except to the extent that the infrastructures simultaneously serve both the military and civilian sectors. Thus, the urge to strike at targets that will damage civilians (mostly in the economic and environmental senses, but including some incidental losses of life) may prove irresistible. In many ways, information warfare affords the opportunity to achieve the coercive goals that Douhet and De Seversky associated with strategic air bombardment—minus the bloodshed. Indeed, strategic information warfare appears to lie somewhere between airpower and economic sanctions on the spectrum of tools of suasion. It can be far more disruptive and costly to an adversary than an economic embargo but is less destructive than bombing—characteristics that may make it a very attractive policy option.

But the ease of engaging in and the attractiveness of information warfare must be weighed, for the purpose of policy analysis, against both the ethical and practical concerns. The ethical problem is clear: A significant aspect of information warfare aims at civilian and civilian-oriented targets; also, despite its negligible lethality, it nonetheless violates the principle of noncombatant immunity, given that civilian economic or other assets are deliberately targeted. In addition to the ethical dilemma posed by information warfare, there is the practical problem that whoever might begin the business of striking at civilian-oriented targets would be inviting retaliation in kind—both from nation-states and from individuals or small groups that are armed with advanced information technology.

The problem is akin to that of the issue of the aerial bombing of cities, as conceived of in the 1920s and 1930s. The air powers of the day were in general agreement—once it grew clear that many would have this capability—that they would avoid striking at each others' cities. Indeed, with only a few exceptions, the warring states at the outset of World War II strove to refrain from deliberately bombing civilian targets.[22] Indeed the circumstances that sparked a shift, leading to the London Blitz and the Royal Air Force's retaliatory fire bombings of German cities were accidental.[23] However, once the shift was made, all combatants went about the business of civilian targeting with a will, culminating in the nuclear attacks on Hiroshima and Nagasaki. The trend of targeting civilians deepened, if anything, in the Korean War, at the end of which only one undamaged building stood in all Pyongyang.[24] But today's technologies are refining the accuracy of air bombardment, making it possible to craft campaigns that do far less damage to civilians or civilian-oriented targets.

[22] The German *Luftwaffe's* bombings of Warsaw and Rotterdam, the early exceptions, were nevertheless circumstances in which both cities formed part of active enemy resistance to advancing German forces, and held substantial military assets within their boundaries. On these bombings, see Bekker (1968), pp. 55–57, 100–114. On the accidental end of the "no-capital-cities" bombing convention in World War II, see Legro (1995), pp. 134–141.

[23] This had do with a German pilot inadvertently jettisoning his bombs over London when he thought he was elsewhere. Although this "accident" spurred the Germans to begin bombing British cities, senior *Luftwaffe* leaders had been arguing for this expansion of the campaign as a means of forcing the British Royal Air Force to come out and grapple with German fighters. On this, see Keegan (1989), p. 96.

[24] Hastings (1987), p. 268, notes: "Installations in Pyongyang were hit again by massed bomber raids in July and August [1952]. . . . Pyongyang had been flattened, hundreds of thousands of North Korean civilians killed."

No such technological solution appears imminent in the realm of information warfare. There is rather the problem of a diffusion of attack capabilities to many actors who may have the capability to mount precise attacks, but perhaps have little incentive to limit their aggression. This implies a practical need to find ways to discourage attacks on civilian-oriented targets. From a policy perspective, there is an initiative that a leading information power, such as the United States, might take: adopting a declaratory doctrine of "no first use" of information warfare against largely civilian targets. It is a simple, straightforward step, but one that nevertheless still allows for information-warfare strikes against military-oriented targets (e.g., operations centers, logistics, and command and control nodes).[25] Further, it allows retaliation in the event that one's own civilian targets have been hit (presuming that the attacker's identity can be ascertained).

The problem of ambiguity regarding information-warfare perpetrators is indeed difficult but is not insurmountable. In the context of war, there is always some purpose to such attacks, and one may add logical inference to the pool of other detection resources in parsing out just who is behind the attacks in question. This may mitigate the problem of ambiguity, which existed in earlier eras—and has been coped with effectively. A good example of dealing with ambiguity is the "phantom" submarine attacks on merchant ships bringing aid to the Loyalists during the Spanish Civil War (1936–1939). Britain quickly inferred that the Italians, supporters of the Fascists, were likely suspects behind these attacks; a retaliatory threat was soon made, despite Italian denials of culpability. The British remained firm, asserting that the Italians would be struck unless the attacks were halted. The "phantom pirate" attacks stopped immediately and never resumed.[26]

[25] It is the same, in many respects, as the notion of no first use in the nuclear context. However, in the nuclear setting, this type of restraint was thought to increase the risk of the outbreak of conventional war. Because U.S. power today is preponderant, it is hard to conceive of a no-first-use pledge for information warfare as having the effect of undermining the deterrence of conventional war. The nuclear no-first-use debate is neatly exposited in two short essays. For the view in favor of no first use, see Bundy et al. (1982). The rebuttal soon followed, from Kaiser et al.(1982).

[26] See Thomas (1961), pp. 475–476, who notes that the British retaliatory threat went beyond attacking phantom submarines in Spanish waters, to include all international waters, even Italian territorial waters. The Italian Foreign Minister, Count Galeazzo

The other potential problem with a no-first-use pledge is that it takes away an attractive coercive tool—the use of information-warfare strikes against a potential aggressor's many infrastructures as a means of signaling or deterring attack in some politico-military crisis. Against this benefit, however, one must weigh the cost of participating in a behavioral regime in which such attacks are tolerated—and that would likely do enormous disruptive harm to the richest set of information targets in the world, which are to be found in the United States. Even with a pledge of no first use against civilian-oriented targets, the option of using information warfare against enemy militaries remains—and, properly employed, might prove to be a good deterrent.

Compared to the problems with crafting policy approaches that will cope with the new dilemmas for noncombatant immunity, which are difficult but not unduly so, the policy alternatives in the realms of "proportionality" and acting in a way that does "more good than harm" seem much less daunting. With regard to proportionality, a number of very straightforward options seem available.

First, a good declaratory position on proportionality might extend to a policy by which information-warfare attacks would engender identical retaliatory response—subject, of course, to proper identification of the perpetrator. However, when the attacker does not have a set of information targets large enough for a proportionate response, or has no information-oriented targets, the retaliation might have to take the form of the use of more-traditional military force against strategic targets of the perpetrator. In this case, proportionality may prove complex in the operational phase.

With regard to doing more good than harm, this aspect of just war theory seems still both useful and feasible. The discriminate nature of information warfare should allow a very careful calibration of effects. The only likely difficulty could ensue in situations in which information-warfare attacks do not have the coercive results envisioned. Indeed, it may prove very difficult to predict the psychological effects of such attacks on either elite decisionmakers or mass

Ciano, in his *Diaries* (1952), pp. 7–8, observed that this threat, along with skillful British diplomatic maneuvering at the Nyon Conference, put an end to the secret Italian campaign.

publics. In this case, if information warfare were used preventively or preemptively and failed in its purpose, it might even be said that an escalation to general war was the fault of taking the information-warfare action in the first place. Therefore, the risks of escalation versus the likelihood that information warfare will head off a conflict must be very carefully assessed before relaxing any notions of "right purpose," "last resort" or "noncombatant immunity."

CLOSING THOUGHTS

The key points to be drawn from this chapter begin with the insight that information warfare may seriously attenuate the ethics of going to war (*jus ad bellum*). Secondarily, though, just warfighting (*jus in bello*) issues seem to retain their currency and value.

Policy toward and doctrinal development of information warfare thus need to focus on the latter area, taking special care to avoid encouraging strikes against civilian-oriented targets but giving less consideration—relatively—to proportionality and doing more good than harm. The last two issues are simply less nettlesome than the burgeoning problem of civilian vulnerability to strategic information warfare.

Information warfare makes war more thinkable. This seems inescapable—and quite troubling. Yet it does not require that waging information warfare be either destructive or unjust. To the contrary, ethical notions of just warfighting will likely continue to provide a useful guide to behavior well into the information age. This poses the possibility of giving an affirmative answer to James Turner Johnson's question (Johnson, 1984) about whether modern war, replete with all its emerging technologies, can ever be just.

REFERENCES

Aldrich, Richard W., *The International Legal Implications of Information Warfare,* Colorado Springs: Institute for National Security Studies, 1996.

Alejandro, Roberto, *The Limits of Rawlsian Justice,* Chicago: University of Chicago Press, 1997.

Aquinas, Thomas, *Summa Theologica*, Chicago: University of Chicago Press, 1952.

Ball, Desmond, and Jeffrey Richelson, eds., *Strategic Nuclear Targeting,* Ithaca, N.Y.: Cornell University Press, 1986.

Bekker, Cajus, *The Luftwaffe War Diaries*, New York: Doubleday, 1968.

Bundy, McGeorge, George F. Kennan, Robert S. McNamara, and Gerard Smith, "Nuclear Weapons and the Atlantic Alliance," *Foreign Affairs*, Spring 1982, pp. 753–768.

Ciano, Count Galeazzo, *Diaries,* London: Methuen and Company, 1952.

De Seversky, Alexander, *Victory Through Air Power,* New York: Simon and Schuster, 1942.

Douhet, Giulio, *The Command of the Air*, Ferrari trans., New York: Coward-McCann, 1942.

Gersonides, Levi, *The Wars of the Lord*, as excerpted in Adam Steinsaltz, ed., *The Essential Talmud*, New York: Basic Books, 1976.

Garrett, Stephen, *Ethics and Airpower in World War II,* New York: St. Martin's Press, 1993.

Hastings, Max, *The Korean War*, New York: Simon and Schuster, 1987.

Hoffman, Bruce, "Responding to Terrorism Across the Technological Spectrum," in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, Calif.: RAND, 1997, pp. 339–367

Johnson, James Turner, *Just War Tradition and the Restraint of War*, Princeton, N.J.: Princeton University Press, 1981.

Johnson, James Turner, *Can Modern War Be Just?* New Haven: Yale University Press, 1984.

Kagan, Donald, *On the Origins of War*, New York: Doubleday Anchor, 1994.

Kaiser, Karl, Georg Leber, Alois Mertes, and Franz-Josef Schulze, "Nuclear Weapons and the Preservation of Peace," *Europa-Archiv*, Vol. 7, Summer 1982, pp. 157–171.

Keegan, John, *The Second World War,* New York: Viking, 1989.

Legro, Jeffrey W., *Cooperation Under Fire: Anglo-German Restraint During World War II*, Ithaca, N.Y.: Cornell University Press, 1995.

Libicki, Martin, *What is Information Warfare?* Washington, D.C.: National Defense University Press, 1996.

Molander, Roger, Peter Wilson, and Andrew Riddile, *Strategic Information Warfare: A New Face of War,* Santa Monica, Calif.: RAND, 1996.

Moore, G. E., *Principia Ethica,* London: Cambridge University Press, [1903] 1993.

Ober, Josiah, "Classical Greek Times," in Michael Howard, Geo. Andreopoulos, and Mark R. Shulman, eds., *The Laws of War: Constraints on Warfare in the Western World*, New Haven: Yale University Press, 1994, pp. 12–26.

Pape, Robert A., *Bombing to Win: Airpower and Coercion in War,* Ithaca, N.Y.: Cornell University Press, 1995.

Quester, George, *Deterrence Before Hiroshima,* New York: John Wiley & Sons, 1966.

Ramsey, Paul, *War and the Christian Conscience: How Shall Modern War Be Conducted Justly?* Durham, N.C.: Duke University Press, 1961.

Rawls, John, *A Theory of Justice,* Cambridge, Mass.: Belknap Press, 1971.

Rosenberg, David Alan, "Nuclear War Planning," in Michael Howard, Geo. Andreopoulos, and Mark R. Shulman, eds., *The Laws of War: Constraints on Warfare in the Western World,* New Haven, Conn.: Yale University Press, 1994, pp. 160–190.

Russell, Frederick H., *The Just War in the Middle Ages*, Cambridge, England: Cambridge University Press, 1975.

Schelling, Thomas C., *Arms and Influence,* New Haven, Conn.: Yale University Press, 1966.

Schwartau, Winn, "Ethical Conundra of Information Warfare," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., *Cyberwar: Security, Strategy and Conflict in the Information Age*, Fairfax, Va.: AFCEA International Press, 1996, pp. 243–249.

Steinsaltz, Adam, *The Essential Talmud*, New York: Basic Books, 1976.

Thomas, Hugh, *The Spanish Civil War*, New York: Harper & Brothers, 1961.

Thomas, Tim, "The Threat of Information Operations: A Russian Perspective," in Robert Pfaltzgraff and Richard Shultz, eds., *War in the Information Age: New Challenges for U.S. Security*, London: Brassey's, 1997.

Thucydides, *The History of the Peloponnesian War*, New York: Everyman's Library, 1938.

Tsymbal, V. I., "Concepts of Information Warfare," a speech presented at the conference on Evolving Post–Cold War National Security Issues, held in Moscow, September 12–14, 1995.

Walzer, Michael, *Just and Unjust Wars*, New York: Basic Books, 1977.

Warden, John, *The Air Campaign*, London: Brassey's, 1989.

Williams, Phil, "Transnational Criminal Organisations and International Security," *Survival*, Vol. 36, No. 1, Spring 1994, pp. 96–113.